

Application No.: 09/463,907

Docket No.: 20162-00547-US

**REMARKS**

The Office Action and prior art relied upon have been carefully considered.

Claim 6 was rejected under 35 U.S.C. § 102(b) as being anticipated by Kim et al. (U.S. Pat. No. 5,796,837). The remaining claims 1-3, 8-11, 13-16, 18-23, 25-29 and 31-38 stand rejected under 35 U.S.C. § 103 based on Kim et al. in combination with the cited secondary references.

Regarding paragraphs 6, 7 and 8 of the Office Action, in respect of claim 6, the Examiner has overlooked the feature that the candidate function generating means generates candidate functions each formed by a combination of plural functions of different algebraic structures. This feature is based on the inventor's finding described from page 17, line 27 to page 19, line 22, and is not taught nor suggested by Kim et al.

Regarding the Examiner's paragraphs 9-12, as the Examiner has admitted, in paragraph 12, Kim et al. does not disclose anything about differential-linear cryptanalysis.

The cited Langford et al. reference discloses differential-linear cryptanalysis; however, this reference does not show any resistance evaluation on functions against differential-linear cryptanalysis.

Regarding paragraph 13, "Block Cipher-Analysis, Design and Application" describes of linear cryptanalysis, differential cryptanalysis, etc., but does not describe anything about differential-linear cryptanalysis.

The equation (6.2) referred to by the Examiner represents an evaluation equation for linear cryptanalysis. Also, the equation in column 4, lines 25-30 of the Kim et al. patent relates to evaluation for linear cryptanalysis (see col. 4, lines 10-20). Both equations may correspond to the equation (4) on page 9 of the present application. However, the meaning of the equation (4) completely differs from that of the equation recited in the original claim 2, the features of which are incorporated into amended claim 1.

Application No.: 09/463,907

Docket No.: 20162-00547-US

Regarding paragraphs 14 and 15, Kim et al. does not teach anything about evaluation on resistance against differential-linear cryptanalysis recited in claim 1 from which claim 3 is dependent; therefore, claim 3 should be allowed.

Regarding paragraphs 16 and 17, claim 27 corresponds to claim 9 which includes the feature of evaluating resistance against differential-linear cryptanalysis; therefore, claims 16 and 17 should be allowed.

Regarding paragraphs 18-25, since claim 6 is considered to be allowable, claim should be allowable. Claim 13 is amended to incorporate the feature of claim 19, whereby a composite function is used as the candidate function. Claim 20 is also amended to incorporate the feature of claim 26, whereby a composite function is used as the candidate function.

Regarding paragraphs 26-32, claims 13 and 20 are amended to incorporate the feature of using composite functions as the candidate functions. This feature is not taught in any cited reference.

Regarding paragraphs 33-35, claims 14 and 21 are dependent from claims 13 and 20, respectively, and therefore, should be allowed.

Regarding paragraph 36, claims 15 and 18 are dependent directly or indirectly from claim 13, and therefore should be allowed.

Regarding paragraph 37, claims 19 and 26, the features of which are incorporated into claims 13 and 20, respectively, are cancelled.

Regarding paragraphs 38-43, claims 33, 35 and 37 are dependent from claims 1, 9 and 27, respectively, and therefore should be allowed.

Regarding paragraphs 44 and 45, claims 34, 36 and 38 are dependent from claims 33, 35 and 37, respectively, and therefore should be allowed.

Application No.: 09/463,907

Docket No.: 20162-00547-US

In summary, the present amendment places all of the remaining claims in condition for allowance.

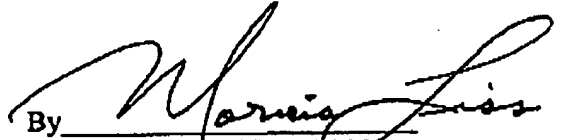
In view of the above, each of the presently pending claims in this application is believed to be in immediate condition for allowance. Accordingly, the Examiner is respectfully requested to pass this application to issue.

Applicant believes no fee is due with this response. However, if a fee is due, please charge our Deposit Account No. 22-0185, under Order No. 20162-00547-US from which the undersigned is authorized to draw.

Dated:

10/28/04

Respectfully submitted,

By   
Morris Liss, Reg. No. 24,510  
CONNOLLY BOVE LODGE & HUTZ LLP  
1990 M Street, N.W., Suite 800  
Washington, DC 20036-3425  
(202) 331-7111  
(202) 293-6229 (Fax)  
Attorneys for Applicant